Board of Governors of the Federal Reserve System

AUDIT OF THE BOARD'S INFORMATION SECURITY PROGRAM

OFFICE OF INSPECTOR GENERAL

(A0106)

September 2001

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

OFFICE OF INSPECTOR GENERAL

September 28, 2001

The Honorable Roger W. Ferguson, Jr.
Vice Chairman and Administrative Governor
Board of Governors of the Federal Reserve System
Washington, DC 20551

Dear Vice Chairman Ferguson:

We are pleased to present our *Report on the Audit of the Board's Information Security Program* (A0106). We performed this audit pursuant to the Government Information Security Reform Act (Security Act) which requires each agency Inspector General to conduct an annual independent evaluation of the agency's information security program and practices. This was the first year that such evaluations were required; similar evaluations are to be conducted next year with Congress expected to make a judgment as to whether they will be required thereafter. Our specific audit objectives, based on the Security Act's requirements, were to evaluate the effectiveness of security controls and techniques for selected information systems and to evaluate compliance by the Board of Governors of the Federal Reserve System (Board) with the Security Act and related information security policies, procedures, standards, and guidelines.

Overall, we found that the Board's information security program is generally effective. Our security control tests did not identify any major security control weaknesses, although we found that controls needed to be strengthened in several areas. We provided our test results to management under separate restricted cover and we plan to follow up on implementation of our recommendations as part of our future audit activities related to the Board's implementation of the Security Act.

Although the Board's information security program is generally effective, we found that the Board has not yet achieved full compliance with the Security Act's requirements. The Board follows the Federal Reserve System's *Information Security Manual* (ISM) which contains a set of general guidelines regarding information security. Although we found the majority of the Security Act's requirements are covered by the ISM, several key aspects of the Security Act are either not addressed or are addressed to a limited extent. Specific areas where we believe additional guidance is required are clearly defining roles and responsibilities, developing security plans, enhancing annual security control reviews, and responding to security-related incidents. We also believe additional opportunities exist to enhance the Board's information security program relating to security awareness and training and to the risk assessment process.

Our first five recommendations are designed to help bring the Board into compliance with the Security Act's requirements and better position the Board to conduct next year's program reviews. Our first two recommendations (about more clearly defining roles and responsibilities) represent a shift from the Board's decentralized approach to implementing its Boardwide information security program to an approach that centralizes oversight and enforcement authority with the Board's Chief Information Officer. We believe, however, that such a shift is necessary to provide effective oversight of the Board's information security program in light of the Security Act's requirements. Our next three recommendations represent areas where we believe additional guidance is required. We have suggested that the guidance described in these recommendations be included in a Board-specific supplement to the ISM. Our final two recommendations address other areas of the Board's information security program that we believe can be further enhanced.

In his written response to the report, the Staff Director for Management generally agreed that our seven recommendations would help bring the Board into compliance with the Security Act and enhance the Board's information security program. The Staff Director's description of actions planned or in process is responsive to the specific issues discussed in our recommendations.

We are providing copies of this report to Board management officials and the report will be added to our publicly available Web site. In addition, the Chairman will provide the report to the Director of the Office of Management and Budget as required by the Security Act and a copy will be provided to the House Committee on Government Reform, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations based on the subcommittee chairman's request. We will also summarize the report in our next semiannual report to the Congress. Please contact me if you would like to discuss the audit report or any related issues.

Sincerely,

Barry R. Snyder
Inspector General

Enclosure

Board of Governors of the Federal Reserve System

AUDIT OF THE BOARD'S INFORMATION SECURITY PROGRAM

OFFICE OF INSPECTOR GENERAL

(A0106)

September 2001

TABLE OF CONTENTS

BACKGROUND

Legislative Requirements

On October 30, 2000, the President signed into law the FY2001 Defense Authorization Act, including Title X, subtitle G, "Government Information Security Reform" (Security Act). The Security Act amends the Paperwork Reduction Act (PRA) of 1995 by enacting a new subchapter on "Information Security" and provides a comprehensive framework to ensure proper management and security of the information resources supporting federal operations and assets. The Security Act codifies existing information security requirements found in Office of Management and Budget (OMB) Circular A-130, Appendix III, and reiterates security responsibilities outlined in other legislation, including the Computer Security Act of 1987, PRA, and the Clinger-Cohen Act of 1996.[1]

The Security Act sets forth specific information security responsibilities for agency officials. The Security Act requires that each agency develop and implement an agencywide risk-based security program to provide information security throughout the life cycle of all systems supporting the agency's operations and assets. The Security Act emphasizes the Chief Information Officer's (CIO) strategic, agencywide security responsibilities, including responsibility for integrating the agency's security plan into the agency's performance plans and into the agency's enterprise architecture and capital planning and investment control processes.

The Security Act also places responsibility on agency officials for assessing the information security risks of the operations and assets for the programs and systems over which they have control. Officials are to determine, based on their risk assessments, the level of information security appropriate to protect such operations and assets and to periodically test and evaluate information security controls and techniques. The Security Act directs the program officials, in consultation with the CIO, to review each agencywide information security program at least annually.

The Security Act also establishes requirements for conducting annual independent evaluations of agency information security programs and practices. The independent evaluations are designed to test the effectiveness of security controls and techniques and to assess compliance with the Security Act's requirements. Responsibility for the independent evaluations has been given to the agency's Inspector General (IG). As required by the Security Act, each agency head is to submit the results of the IG's independent evaluation to the Director of OMB on an annual basis.

The Security Act gives the Director of OMB responsibility for establishing governmentwide polices for the management of information security programs. In January 2001, OMB issued memorandum 01-08 to provide guidance for agencies to implement the Security Act's requirements; the guidance focused on the areas of the legislation that introduced new or

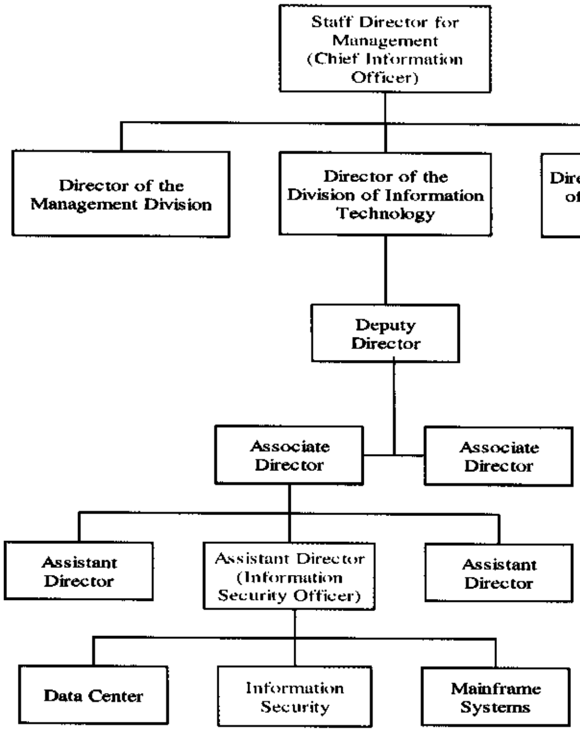
[1] The Legal Division of the Board of Governors of the Federal Reserve System (Board) has previously determined that the Board is not subject to all provisions of OMB Circular A-130 or to the Clinger-Cohen Act of 1996. The Board is, however, subject to PRA and is therefore subject to the requirements contained in the Security Act.

modified requirements and requested that agencies submit the results of their annual program reviews in addition to the independent evaluations. In June 2001, OMB issued memorandum 01-24 which requested agency heads to submit, contemporaneously with submission of the independent evaluations and program reviews, a brief executive summary developed by the agency CIO, agency program officials, and the IG based on the results of their work. In the executive summary, agency officials and IGs are to respond to fourteen topic areas. The responses are designed to provide a general overview of the agency's information security program; discuss specific security program performance; and identify the agency's next steps to correct any security weaknesses identified through the annual program reviews, the independent evaluations, or other reviews and audits. The executive summaries will serve as the primary basis for OMB's summary report to Congress, as required by the Security Act.

Information Security Roles and Responsibilities

The Board of Governors of the Federal Reserve System (Board) has designated the Staff Director for Management as the Board's Chief Information Officer. The Board's Information Security unit, in the Division of Information Technology (IT), is responsible for the security of the Board's automation and telecommunications and for providing consulting support to the Board and the Reserve Banks related to information security and new technology. The unit is also responsible for the Board's security awareness program, computer virus detection, and for providing leadership to the Federal Reserve System (System) for information security projects, including intrusion detection. The Information Security unit reports to an IT assistant director who serves as the Board's Information Security Officer (ISO) and is the focal point for the Board's information security activities. (See organizational chart that follows.)

Board Organizational Chart for Information Security


Staff Director for Management (Chief Information Officer)
Director of the Management Division
Director of the Division of Information Technology
Director of the Division of Support Services
Deputy Director
Associate Director
Associate Director
Assistant Director
Assistant Director (Information Security Officer)
Assistant Director
Data Center
Information Security
Mainframe Systems

Because much of the information technology at the Board is decentralized, each division and office has information security responsibilities. Specifically, network administrators are responsible for configuring, maintaining, and protecting the systems under their control to ensure a secure distributed operating environment. Information owners are responsible for assessing the degree of business risk associated with their systems and applications, classifying and authorizing access to information, and ensuring proper security controls are in place. To assist divisions with these responsibilities, the Board has established an Information Security Committee (ISC) comprised of representatives from each division and office. The ISC functions as a Boardwide coordinating body with responsibility for advising division management regarding System information security strategic direction and initiatives. The ISC is also responsible for the local application of policies and procedures in support of System information security policies and safeguards.

Information Security Guidance

To provide policy direction regarding the protection of its information assets, the System developed the *Information Security Manual* (ISM). The ISM defines policies and safeguards for information security and is applicable to all automated platforms and manual processes used throughout the System. The ISM is built on three security principles: confidentiality (assurance that information is disclosed only to authorized entities), integrity (assurance that information has not been improperly altered), and continuity of operations (assurance that correct information is available when needed).

Two other manuals, the *Distributed Processing Security Support Manual* and the *Mainframe and FEDNET Security Support Manual*, contain policies and procedures specifically related to those information technology environments and support the general guidance provided by the ISM.[2] Board divisions and offices are required to comply with the policies and safeguards in these manuals.

Information Technology Architecture

The Board's information technology architecture includes mainframe and distributed operating environments. The Board relies heavily on its mainframe computer system to process and analyze data used in making monetary and economic policy decisions and in performing its other regulatory, operational, and administrative activities. The majority of the Board's mission-critical systems are mainframe applications, underscoring the need to provide a secure and reliable mainframe processing environment. The Board's mainframe uses an access control software which operates as an extension of the operating system to protect application programs and data against unauthorized destruction, modification, or disclosure. The access control software identifies and authenticates users when they access the computer, protects programs and

[2] The *Distributed Processing Security Support Manual* contains safeguards specific to distributed processing environments, such as PCs, external network connectivity, local area networks, wide area networks, and telephonic systems. The *Mainframe and FEDNET Security Support Manual* contains safeguards specific to mainframe computers using the Multiple Virtual Systems operating system and FEDNET Communications equipment.

data by defining who can use the programs and data and in what way, and logs access attempts. Mainframe operations are IT's responsibility, although Board divisions and offices are considered the data owners.

While mainframe computer operations are used for large-scale processing and storage, the Board has shifted resources to provide analytical tools to users at their desktops. Desktop computing operations give users powerful, cost-effective tools for convenient access and greater control over data. In a distributed environment, however, operational management functions such as security, backup and recovery, and problem resolution may not be as fully developed as for mainframe operations. To address this potential control weakness in the distributed processing environment, the Board relies on the development of effective processes for detecting and controlling distributed processing activities and on establishing appropriate backup and disaster recovery procedures. The Board's distributed processing environment includes Microsoft Windows and UNIX-based servers, personal computers, laptops, and the associated telecommunications infrastructure. IT is generally responsible for distributed hardware, software, and communications, although some divisions maintain their own processing platforms. In a distributed processing environment, Board divisions and offices are still considered the data owners and may also have responsibility as the data custodians.

OBJECTIVES, SCOPE, AND METHODOLOGY

We conducted our audit fieldwork from April to September 2001. Our audit objectives, based on the Security Act's requirements for conducting independent evaluations, were to evaluate the effectiveness of security controls and techniques for selected information systems and to evaluate the Board's compliance with the Security Act and related information security policies, procedures, standards, and guidelines.

To achieve our objectives, we reviewed Board and System documentation pertaining to information security and met with officers and staff throughout the Board with information security responsibilities. To test security controls and techniques, we developed a control test plan based on government and industry guidelines and publications.[3] Our test plan focused on reviewing controls over information classification, user authorization, user access, and security violation detection and reporting. To provide representative coverage across the Board's information technology platforms and mission areas, we selected three applications for review; the following table shows the platform and mission area for each application included in our test. In addition, we reviewed the results of independent testing performed on the Board's public web site and web servers to evaluate actions taken on the recommendations made. We also reviewed the access control software on the Board's mainframe to assess the adequacy of data security-related control objectives and policies, and the associated administrative and operational procedures employed by management to provide logical security over computing resources.

[3] We reviewed guidelines contained in the *Control Objectives for Information and related Technology* (COBIT), the General Accounting Office's *Federal Information System Controls Audit Manual* (FISCAM), and National Institute of Standards and Technology (NIST) publications.

Applications Included in Office of Inspector General (OIG) Control Testing

APPLICATION[4]	PLATFORM	MISSION AREA
Lagged Float	Mainframe	Reserve Bank Oversight
AutoM	UNIX-based Distributed	Monetary Policy
Consumer Affairs Report of Examination Data System (CARES)	Windows-based Distributed	Supervision and Regulation

To evaluate the Board's compliance with the Security Act, we reviewed the policies and procedures in the ISM to determine whether the manual provides a sufficient framework for achieving the Security Act's requirements. We also reviewed the Board's implementation of the ISM, focusing primarily on those areas for which OMB requested a specific response as part of the agency's executive summary. Because the Security Act allows the use of any audit, evaluation, or report related to the agency's security programs and practices, in making our independent assessment, we reviewed prior OIG audit activities relative to information security. (Appendix 1 contains a list of the relevant audit work.) We also reviewed reports prepared by an independent consultant during a 1999 review of the security of the Board's public web site, as well as reports prepared in 1999 and 2001 by the System's Virtual Competency Center related to their independent tests of the Board's information technology architecture. Our audit was conducted in accordance with generally accepted government auditing standards.

FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

Overall, we found that the Board's information security program is generally effective. Our security control tests of three applications and our review of the Board's mainframe access control software and public web site and web servers did not identify any major security control weaknesses, although we found that security controls needed to be strengthened in the areas of access controls and separation of duties. Given the sensitivity of the issues involved, we provided our test results to management under separate restricted cover and we plan to follow up on implementation of our recommendations as part of our future audit activities related to the Board's implementation of the Security Act.

Even though the Board's information security program is generally effective, we found that the Board has not yet achieved full compliance with the Security Act's requirements. Since the ISM serves as the basic policy and guidance document for the Board's security program, we compared the manual with provisions in the Security Act. While we found the majority of the Security Act's requirements are covered by the ISM, several key aspects of the Security Act are

[4] The Lagged Float System collects float data from System check processing centers for analysis. The AutoM application consolidates data from various sources for use in monetary policy calculations. CARES collects and stores data from consumer affairs examinations.

either not addressed or are addressed to a limited extent. Specifically, the ISM does not establish the central, agencywide authority that the Security Act envisions. Although the Staff Director for Management has been designated as the Board's CIO, the Staff Director's roles and responsibilities related to information technology in general—and information security in particular—have never been clearly defined. We also found that the Board's Information Security unit views itself as a service organization with limited authority to enforce the ISM's requirements across all divisions and offices. In addition, the ISO's organizational placement does not allow him to effectively assist the CIO in fulfilling the responsibilities enumerated in the Security Act. We further found that the Board has not developed an agencywide security plan nor has the Board required each program manager to develop a system-specific security plan. While the Board has initiated two application reviews to comply with the Security Act's annual program evaluation requirement, additional guidance is needed to clearly define and track the applications subject to review, report the review results, and develop corrective action plans. We also found that the Board has provided limited guidance to the divisions on incident response; specifically, the Board needs to more clearly define what constitutes a security incident and to identify the procedures for responding to such incidents.

Our first five recommendations are designed to help bring the Board into compliance with the Security Act's requirements and better position the Board to conduct next year's program reviews. The first two of these recommendations are designed to provide the CIO, the ISO, and the Information Security unit with additional oversight and enforcement authority for information security across the Board. We recognize this represents a shift from the Board's decentralized approach to implementing Boardwide programs. We believe, however, that such a shift is necessary to provide effective oversight of the Board's information security program and fully implement the Security Act. Our next three recommendations address developing security plans, enhancing security control reviews, and responding to security-related incidents. We believe that the additional guidance described in these recommendations should be included in a Board-specific supplement to the ISM since the ISM is designed as a System manual that provides general policy and guidance to all System entities. Such a supplement will help ensure that all Board management and staff are aware of their specific information security responsibilities.

We also believe additional opportunities exist to enhance other portions of the Board's information security program. Although the Board has developed a security awareness and training program, there is no annual recertification requirement and the Board has not established specific training expectations for staff with significant security responsibilities. In addition, we believe the Board's risk assessment process can be improved by having the CIO or the ISO review the assessment results to ensure consistency and adherence to ISM standards. Our final two recommendations address these important aspects of information security.

1. We recommend that the Administrative Governor clearly define the roles and responsibilities of the CIO and program officials to encompass all requirements contained in the Security Act.

The Security Act outlines a number of significant security-related responsibilities for individuals within each agency. For example, the Security Act defines the CIO as having responsibility for providing a strategic view of the agency's architecture and crosscutting security needs. The Security Act directs agency CIOs to develop, implement, and maintain an agencywide security program and to describe the program in detail in an agencywide security plan. The CIO is also to participate in developing agency performance plans to establish the budget, staffing, training resources, and time periods required to implement the security program. The CIO must also ensure that agency security programs are fully integrated into the agency's enterprise architecture and capital planning and investment control processes. In addition, the CIO is to work with agency program officials in reviewing the information security program on an annual basis.

Since the Security Act essentially codifies many of the requirements contained in OMB Circular A-130, many federal agencies may already have clearly defined these responsibilities. The Board, however, has never updated its policy and guidance to specify what is expected of its Chief Information Officer. In June 1999, the Administrative Governor designated the Staff Director for Management as the Board's CIO. The designation memorandum did not, however, delineate any specific responsibilities or set any expectations. In addition, the Board's official delegations have not been updated to include CIO-related functions. Although the Staff Director is fulfilling the CIO function for the Board and has taken steps to implement the Security Act's requirements, we believe that clearly defining the CIO's specific information security roles and responsibilities is important given the significant, agencywide responsibilities the Security Act establishes for this position. We believe the delegation should not only provide for the CIO as a focal point for disseminating information security policy and guidance, but the delegation should also give the CIO direct oversight responsibility to ensure the guidance is implemented in an efficient and effective manner. We believe this oversight function is important both to help implement new information security requirements (such as developing security plans and performing controls reviews), and to enhance portions of the Board's existing security program (such as security awareness and training and conducting risk assessments).

The Security Act also identifies specific responsibilities for agency program officials.[5] Each program official is to develop, implement, and maintain a security program (and document it in a security plan) that assesses the risk of, and provides adequate security for, the operations and assets of programs and systems under his or her control. Agency program officials should also periodically test and evaluate information security controls and techniques for their programs and systems.

We found that the ISM already assigns program officials the responsibility for performing some of these functions. Specifically, the ISM addresses performing information security risk assessments, ensuring appropriate security controls are in place, and conducting periodic security-control reviews that focus on the adequacy of and compliance with information security policies. The ISM does not, however, include requirements for developing system-specific security plans nor does the manual specify the frequency, scope, or reporting requirements for the security control reviews. In addition, for the applications we reviewed as part of our control testing, we found that periodic security control reviews had not been conducted. We believe that additional guidance in these areas would help ensure program officials fulfill their responsibilities under the Security Act, and also provide for a stronger information security program at the Board.

[5] At the Board, program officials are generally synonymous with division directors.

2. **We recommend that the CIO (a) clarify the roles and responsibilities of the ISO, the Information Security unit, and the ISC in light of the Security Act's requirements, and (b) reevaluate the ISO's organizational placement.**

The Security Act directs the CIO to designate a senior agency information security official who shall report to the CIO or a comparable individual within the agency. Although not specifically discussed in the Security Act, other related guidance indicates that the ISO's responsibilities should include reporting to the CIO on the implementation and maintenance of the agency's information security program and policies. Because the CIO has information technology responsibilities beyond information security, the ISO will likely become the focal point in many agencies for implementing the Security Act's requirements. Fulfilling this responsibility will, in our opinion, require the ISO to possess a strategic, agencywide perspective with specific cross-cutting responsibilities and strong senior management support.

The Board's ISO currently has direct responsibility for the Information Security unit and serves as the focal point for information security activities at the Board. The ISO also chairs the ISC, which includes representatives from all divisions and offices and functions as a Boardwide coordinating body for the local application of System policies and procedures. We believe these three entities—the ISO, the Information Security unit, and the ISC—form the basic organizational framework that can assist the CIO in fulfilling the Security Act's requirements. The CIO will, however, need to more clearly define the roles and responsibilities of each of these entities to provide them with the necessary strategic perspective and operational direction. We found, for example, that the Information Security unit views itself as a service organization with a reactive—rather than proactive—approach to areas such as new application development and a limited role in enforcement activities such as conducting control reviews or reviewing risk assessments for compliance with the ISM. We also found that the ISC has met infrequently during the past year and has relied on other Board groups to discuss information security issues.

We are concerned that the ISO is not properly positioned within the Board's organizational structure to effectively carry out these responsibilities. Rather than reporting to the CIO or another senior official (as prescribed by the Security Act), the Board's ISO is four organizational levels removed from the CIO (see previous organizational chart). In addition, the ISO has other significant information technology related responsibilities, including the responsibility for the Board's data center and for support of the Board's mainframe operations. Implementing the Security Act's requirements (to include developing security plans, conducting security control reviews, and building a comprehensive incident response program) will, at least initially, require a significant investment of time by the CIO and the ISO to provide necessary guidance and review program results. In addition, the increased oversight and enforcement responsibilities that we envision the CIO investing in the ISO to facilitate implementing our remaining recommendations may run counter to the Board's traditional decentralized management approach, and we believe that the ISO's placement within IT will hamper the ISO's effectiveness. These additional responsibilities could also create a conflict of interest with the ISO's operational functions.

One option would be for the CIO to realign the security function as part of the Office of the Staff Director for Management (OSDM), thus providing a direct reporting relationship to the CIO. In doing so, the CIO will need to ensure that the operational functions currently performed by the ISO and the Information Security unit remain within IT to provide a proper separation of oversight and operational responsibilities. Placing the information security function within the OSDM will also permit the CIO to determine whether other Board security functions should be consolidated. We found, for example, that the Security Section in the Division of Support Services has responsibility for administering the Board's information security program, including the protection of classified proprietary and national security information from unauthorized disclosure. Although this function pertains primarily to printed information, there may be some economies and efficiencies gained by aligning all information security functions in one office.

3. We recommend that the CIO develop an agencywide information security plan and establish guidance for program officials to develop system-specific security plans.

As outlined in the Security Act and subsequent guidance, agency CIOs are to develop, implement, and maintain an agencywide security program that assesses risk and provides adequate security for the operations and assets of all agency programs and systems. The information security program should be documented in an agencywide security plan. In addition, the guidance requires program officials to develop a security plan for each system under their control. The system security plans should be based on the agencywide plan, provide an overview of the system's specific security requirements, and describe the controls in place or planned for meeting those requirements. System security plans should delineate the responsibilities, expected behavior, and required training of all individuals who access the system, and describe appropriate controls for interconnection with other systems.

We found that the Board's CIO has not developed an agencywide information security plan nor has the CIO required each program official to develop a plan tailored to the system or application under his or her control. We recognize that the Board heretofore used the ISM as the basic guidance document for its information security program, and we found that the manual contains some elements of a security plan such as describing the application's work processes and identifying some input, output, and access controls. We also recognize that additional elements of system-specific security plans may exist in other documents, such as system user manuals, risk assessments, and continuity of operations plans. None of these documents, however, contain all aspects of a security plan as outlined in various guidance documents such as OMB Circular A-130 or NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems.*

To achieve compliance with this provision of the Security Act and provide a Board-specific security blueprint, we believe the CIO should develop a separate Boardwide security plan using the ISM as a frame of reference. Rather than simply restate the ISM, however, the plan should reflect the Board's information technology architecture, its organizational structure, and those requirements unique to the Board (such as compliance with federal laws and regulations) that are not found in other System entities. Once the Board's security plan is established, the CIO should provide guidance to the program officials for developing system-specific plans and ensure that the plans are completed in accordance with the established guidance. The systems plans should reflect input from the information owners, system managers, and the information security staff to ensure all perspectives are adequately addressed.

4. **We recommend that the CIO enhance the security control reviews by (a) clearly defining major Board applications, (b) establishing a mechanism to track applications and associated reviews, (c) reviewing test plans and results, and (d) providing guidance for establishing corrective action plans.**

The Security Act requires each agency to review their information security program at least annually. The Security Act also requires agency officials to periodically test and evaluate information security controls and techniques for the systems under their control. As stated in the June 2001 OMB guidance, these system reviews are essential elements of each agency's annual program review. Conducting periodic system reviews is not a new requirement for most federal agencies. OMB Circular A-130, Appendix III, already requires periodic reviews of security controls for an agency's general support systems and major applications.[6] The scope and frequency of these reviews should be commensurate with the risk and magnitude of harm that could occur from threats and vulnerabilities, although the circular generally requires reviews to be conducted at least every three years.

We found that the Board has not conducted the types of reviews described in OMB Circular A-130. Although the ISM requires management to conduct periodic security reviews that focus on the adequacy of, and compliance with, information security policies, these reviews have generally not been conducted. IT management told us that they perform control reviews during application development and informally present the results to the application developers. These reviews are limited, however, to applications developed by IT staff and are not periodically conducted once an application is developed.

Earlier this year, the CIO issued guidance requiring divisions to conduct a review of the security controls for each major application under their control. The guidance directed that the reviews be conducted at least every three years. The CIO suggested that divisions initially focus on applications classified as "mission critical" during Y2K, although the CIO noted that applications other than those deemed mission critical may be classified as major. The CIO also provided a description of the areas to be included in the security reviews. The CIO did not, however, provide specific testing requirements for general support systems, other than to note that IT is responsible for most of these systems at the Board.

Although the CIO's guidance provides a starting point for compliance with the Security Act's periodic testing requirement, we believe that additional guidance is necessary to ensure the Board fully complies with this provision of the Security Act. First, the CIO should establish specific criteria for defining major applications to ensure a consistent interpretation Boardwide.

[6] General support systems are defined in the circular as an interconnected set of information resources under the same direct management control and which share common functionality. General support systems could include a local area network, a communications network, or a data processing center. A major application is defined as an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application.

While we agree that focusing on mission-critical applications provides a good beginning, we are concerned that without additional guidance, divisions will not conduct testing on other significant Board applications. To facilitate scheduling and tracking the control reviews, we believe the CIO should work with all divisions and offices to develop a complete list of major applications for the Board. The list should include the application's data owners, the data custodians, the classification of information processed by or stored in the application, the date of the last risk assessment, and the date of the last security control review.

Once the first tests are completed, the CIO should review the test plans and test results to ensure the scope and methodology are consistent with the requirements of the Security Act and OMB Circular A-130, and then provide any necessary guidance for conducting future control tests. The CIO should also review the test results to identify any systemic vulnerabilities or weaknesses or to note any best practices that should be shared with all program managers. In addition, the CIO should provide guidance to the program managers for developing action plans to correct any weaknesses identified during the reviews. Information regarding corrective action plans must be submitted to OMB by October 31, 2001, and should include the timeframes and resources necessary to implement corrective actions.

5. **We recommend that the CIO develop guidance that more clearly defines a "security incident" and establish Boardwide procedures for incident reporting.**

The Security Act reiterates existing guidance that all agency security programs should include procedures for detecting, reporting, and responding to security incidents. The intent of the Security Act's security incident provision is to ensure that each agency has both the technical and procedural means in place to detect and appropriately report security incidents and share information on common vulnerabilities. All agency security programs are to include policies and procedures that remove unnecessary internal obstacles for timely reporting of security incidents to the appropriate agency authorities, as well as to law enforcement authorities and other external organizations.

The System recently established a National Incident Response Team to play a leading role in System efforts to protect information systems and data resources against unauthorized use and from external attacks. The Federal Reserve Bank of New York (FRB NY) heads the response team and is responsible for establishing Systemwide response procedures. FRB NY is also responsible for determining what, if any, external reporting of security incidents is appropriate. An individual in the Information Security unit serves as the Board's liaison to the System's response team. IT management told us that the Board would report any security incidents to the System's response team. We also note that the Board has established a Virus Response Team with responsibility for recovering from and reporting on computer virus incidents.

Because the System's response team is still in the formulation stages, specific guidance and response procedures have not yet been developed. Although the Information Security unit has prepared incident reporting procedures for Board operations, the procedures apply only to automation resources managed by IT. The procedures do not address the responsibilities of other divisions for identifying or reporting a security incident nor do the procedures discuss external reporting requirements. Although the ISM provides some additional guidance, the guidance does not clearly define what constitutes a security violation or establish to whom the violation is to be reported.

We believe the CIO should develop specific guidance covering the Board's incident response program. The guidance should clearly define what constitutes a security incident, establish response procedures for all divisions, and be disseminated to all staff. Our discussions with IT management and security staff indicated that the focus of incident response is on virus detection and other external threats. We believe the definition of an "incident" should be broader and include internal incidents such as unauthorized attempts to access, alter, or disseminate programs, applications, or the associated information. The procedures should cover notifying and consulting with Board staff, the System's response team, the OIG, other law enforcement officials, and other offices and authorities such as the General Services Administration's Federal Computer Incident Response Capability. (The latter is a requirement of the Security Act.).

6. **We recommend that the CIO enhance the Board's security awareness and training program by (a) requiring all staff to complete an annual security refresher course, (b) establishing additional proactive measures to promote security awareness, (c) establishing specific training requirements for all staff with information security responsibilities, and (d) developing a tracking mechanism to ensure that information security training requirements are met.**

The Security Act requires the agency CIO to ensure the agency has personnel sufficiently trained in their security responsibilities to assist the agency in complying with the requirements of the Security Act and related policies, procedures, standards, and guidance. The Security Act also requires agency security programs to include security awareness training to inform personnel of relevant information security risks and their responsibilities to reduce such risks. These requirements reiterate those of the Computer Security Act of 1987, which specifically requires each agency to provide mandatory periodic training in computer security awareness and accepted computer security practice to all employees involved with the management, use, or operation of a federal computer system. The General Accounting Office noted in its *Federal Information System Controls Audit Manual* that the leading organizations they studied considered security awareness to be one of the most important factors in the overall risk management process.

The ISM contains general requirements for maintaining a security awareness and training program. The ISM's minimum requirements include security awareness training for all new employees and periodic awareness training for individuals handling information resources. The ISM also requires periodically providing job-related information security training, such as basic access control software requirements, password control, risk assessment training, separation of duties, and virus detection and prevention.

In keeping with the ISM requirements, the Board's security awareness program consists of training new employees during initial employee orientation and posting periodic articles on "Inside the Board" related to computer viruses and other information security issues. During initial employee orientation, each employee receives a briefing on physical and information security, including contingency operations, virus information, password construction, and the

Board's Internet permissible use policy. To reinforce security awareness, the ISO periodically posts articles to "Inside the Board" related to a variety of information security topics such as virus alerts, password requirements, and Internet usage. We also found that IT's internal web page on the Board's Intranet contains a link to an "Annual Information Security Statement." The statement is an annual reminder of staff responsibilities regarding the safeguarding of information and physical assets of Board and System computer systems. The statement, which is discussed during new employee orientation, also reminds employees that everyone is responsible for adhering to ISM policies and safeguards and provides a link to the ISM and other security-related guidance.

While the items discussed above are effective methods of educating and updating staff on information security requirements, we believe that the Board's security awareness program can be strengthened in several areas. Although the "Annual Information Security Statement" has been added to new employee orientation, employees who have been at the Board for awhile may be unaware of its existence. In addition, we believe that each employee should be required to acknowledge, in writing, that they have read and that they understand the Board's information security requirements and that they are aware of the penalties for failing to comply. We found that one division (the Division of Consumer and Community Affairs) has established an internal revalidation program for information security. Annually, the division's employees are required to sign a revalidation form acknowledging that they agree to adhere to the ISM's policies and procedures and use the Board's network and networked services in accordance with Board standards. We believe this type of revalidation should be expanded Boardwide and that the ISO or the division's representative to the ISC should collect these statements to ensure that they are completed by all staff.

We also believe that the ISO should consider other methods to promote security awareness. The ISO should, for example, develop an annual refresher training course that employees complete prior to signing the revalidation form. This process would be similar to the annual ethics training conducted by the Legal Division. The ISO should also use less formal methods—such as posters, puzzles, or giveaways—to sustain employee interest in security awareness.

In addition to enhancing security awareness training for all staff, we believe the CIO should develop a security training program for those individuals with specific information security responsibilities. We found that the Board has not identified specific training requirements for individuals throughout the Board with information security responsibilities. The divisions we spoke with identify the training courses they believe are appropriate and stated that most information technology related classes or conferences contain certain elements of information security. We believe, however, that establishing a benchmark will help promote consistency and ensure the Board maintains a high-quality, security-conscious technology staff. The training should also cover the Security Act's requirements to help program managers fulfill their responsibilities under the Security Act. We note that the Security Act directs the Office of Personnel Management (OPM) to review and update OPM regulations and guidance concerning computer security training and the Board should incorporate these guidelines in its training program once the guidance is updated.

To help ensure that the requirements are met, we believe the CIO should establish a mechanism for tracking information security related training. Although divisions such as IT already maintain internal methods of identifying training courses for their staff, there is no central mechanism to track this information. At our request, the training specialist in the Management Division's Human Resources Function provided us with a list of information technology courses taken by Board staff; however, the list was not complete and did not specifically identify those courses with an information security component.

7. **We recommend that the CIO enhance the Board's risk assessment program by ensuring that periodic risk assessments are conducted in compliance with ISM requirements.**

The ISM states that risk assessments must be performed for all Board business functions to identify applicable security policies and safeguards. The ISM also states that risk assessments should be periodically updated and revised, as needed, for any operational changes. While the ISM states that business managers are responsible for ensuring that risk assessments are performed, the manual is silent about the frequency with which updates of the risk assessments are to occur. The ISM also contains no requirement for the business managers to report on the results of the risk assessments.

Earlier this year, the CIO issued guidance to all Board divisions requiring that risk assessments for each functional area be updated and that each division director provide a report to the CIO stating that the risk assessments are current. While this provides the CIO with assurance that the assessments are up-to-date, we believe that requiring the assessments themselves to be submitted would provide greater assurance that not only are they current but that they have been completed in accordance with the ISM. The CIO or the ISO should review the assessments as they are completed to promote consistency, identify common vulnerabilities, and then provide any additional guidance as required. In addition, the CIO should revise the current policy to establish the minimum requirements for updating the assessments. During our audit, IT management told us that going forward, business managers will be required to update their assessments at least every three years. Unless there are significant changes to a program area that would affect the associated threats and vulnerabilities, we believe that three years is a reasonable timeframe. This timeframe would also conform to requirements in OMB Circular A-130.

ANALYSIS OF COMMENTS

We provided a draft copy of this report to the Staff Director for Management for review and comments. His response is included as appendix 2 to this report. The response indicates general agreement with the seven recommendations and discusses actions that have been or will be taken to implement the recommendations. The Staff Director's description of actions planned or in process is responsive to the specific issues discussed in our report and we will follow up on the Board's implementation of our recommendations as part of our future audit work pertaining to the Security Act.

APPENDIXES

Appendix 1 - Prior OIG Audit Activities Pertaining to Information Security

In making our independent assessment, we reviewed OIG audit activities completed during the past two years including our:

- Audit of the Division of Consumer and Community Affairs Distributed Processing Environment and related follow-up work

- Audit of the Division of Reserve Bank Operations and Payment Systems' Distributed Processing Environment and related follow-up work

- Review of Compliance with the Information Security Manual

- Review of the Board's Implementation of Critical Infrastructure Protection

- Monitoring Effort of the Board's Implementation of the Endeavor Change Control Project

Appendix 2 – Division's Comments

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

STEPHEN R. MALPHRUS
STAFF DIRECTOR FOR MANAGEMENT

DATE: September 28, 2001

TO: Barry Snyder

FROM: Steve Malphrus

SUBJECT: Comments on *Report on the Audit of the Board's Information Security Program* (A0106)

We appreciate the opportunity to comment on the draft *Report on the Audit of the Board's Information Security Program* (A0106). Our comments follow each recommendation.

1. **We recommend that the Administrative Governor clearly define the roles and responsibilities of the CIO and program officials to encompass all requirements contained in the Security Act.**

Response: We concur. Under the policies and procedures enumerated in the FR System's information security policy, the Board has a decentralized approach to implementing information security. While effective, we will strengthen our program through centralization of program management to fully comply with the requirements of GISRA.

2. **We recommend that the CIO (a) clarify the roles and responsibilities of the ISO, the Information Security Section, and the ISC in light of the Security Act's requirements, and (b) reevaluate the ISO's organizational placement.**

Response: We concur. We believe that there is value in educating employees regarding roles and responsibilities for information security. More frequent employee education as required by the Security Act should strengthen the Board's "information security culture." We will also reevaluate the placement and reporting of the Board's Information Security Officer (ISO). While we believe that the Security Act's requirements are generally accomplished through the current reporting relationship, we will reevaluate with the Inspector General the ISO's placement.

3. **We recommend that the CIO develop an agency-wide information security plan and establish guidance for program officials to develop system-specific security plans.**

Response: We concur. The Board has an agency-wide security program as enumerated in the Federal Reserve's *Information Security Manual* (ISM). There are, however, requirements of the Security Act that are not part of the *ISM*. It is important to recognize that the Security Act and National Institute of Standards and Technology guidance assume that agencies do not have a comprehensive set of policies and procedures similar to the *ISM* or a strong culture of information security. A key in going forward is to balance compliance benefits and the cost burdens.

Appendix 2 – Division's Comments (con't)

4. **We recommend that the CIO enhance the security control reviews by (a) clearly defining major Board applications, (b) establishing a mechanism to track applications and the associated reviews, (c) reviewing test plans and results, and (d) providing guidance for establishing corrective action plans.**

Response: We concur. Clearer definitions and tracking tools will likely be helpful in ensuring that the Board fully complies with the Security Act.

5. **We recommend that the CIO develop guidance that more clearly defines a "security incident" and establish Boardwide procedures for incident reporting.**

Response: We believe that guidance from Federal Reserve System's recently established National Incident Response Team will be adequate. We agree that the CIO should ensure that divisions understand their responsibilities in identifying and reporting a security incident. We will continue to report incidents to responsible federal authorities.

6. **We recommend that the CIO enhance the Board's security awareness and training program by (a) requiring all staff to complete an annual security refresher course, (b) establishing additional proactive measures to promote security awareness, (c) establishing specific training requirements for all staff with information security responsibilities, and (d) developing a tracking mechanism to ensure that information security training requirements are met.**

Response: We concur. The Federal Reserve has a strong culture of security awareness and has been cited by the GAO as "best practice" organization for risk assessments. While Board employees demonstrate a high degree of information security awareness through their daily activities, such as choosing strong passwords and keeping viruses out of internal networks, the Security Act requires ongoing security awareness training. We will develop a technique to deliver the training in a way that is effective but not unduly burdensome.

7. **We recommend that the CIO enhance the Board's risk assessment program by ensuring that periodic risk assessments are conducted in compliance with ISM requirements.**

Response: We concur. The costs and benefits of periodic risk assessments must be balanced. We will perform periodic assessments and then evaluate the benefits.

Appendix 3 - Principle Contributors to this Report

William Mitchell, Program Manager and Auditor-in-Charge

Ronald Braciak, EDP Auditor

Ariane Ford, Auditor

Lori Jackson, Auditor

Robert McMillon, EDP Auditor